

Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 11 October 2005 Meeting

GSA; 1800 F Street; Training Room; Washington, DC

A. AGENDA

- 1) Welcome & Opening Remarks / Introductions
- 2) Discussion /Vote on Minutes from 13 September FPKIPA meeting
- 3) Results of Electronic Voting
 - a. Approval Vote on 9 August 2005 FPKIPA Minutes
 - b. Approval Vote for EGCA Certificate Policy Change Proposal: 2005-02
 - c. Approval Vote for Revised Charter
 - d. Approval Vote for Wells Fargo MOA at Basic LOA
- 4) Approval Vote for the Revised Certificate Profile
- 5) Approval vote for GPO Cross-Certification at Medium LOA
- 6) FPKI Certificate Policy Working Group (CPWG) Report
 - a. Vote to Approve Mapping Wells Fargo at Medium Hardware Commercial Best Practices
 - b. Discuss Mapping Adobe in 3647 Format
 - c. Discuss CPWG participation by agencies
- 7) FPKI Operational Authority (FPKI OA) Report
 - a. Status of FBCA/Applicant Cross-Certification Technical Testing
- 8) Other Topics
 - a. Wells Fargo Liability Language (context: Medium & Medium Hardware Cross-Certification)
 - b. Document Control
 - c. EGCA Certificate Policy Change Proposal: 2005-03 – Distinguished Name
- 9) Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting started with a quorum of 9 members, including three proxies, and another member joined later.

Organization	Name	Email	Telephone
Department of Commerce (NIST)	Polk, Tim		
Department of Defense	Hanko, Dave		
Department of Energy	Absent		
Department of Health & Human Services (Proxy to Department of Commerce)	Absent		
Department of Homeland Security	Absent		
Department of Justice	Absent		
Department of State	Caldwell, Sally		
Department of the Treasury	Schminky, James		
GSA	Temoshok, David		

Organization	Name	Email	Telephone
NASA (Proxy to DoD)	Absent		
OMB (Proxy to HHS/DOC)	Absent		
USDA/NFC ¹	Goodwin, Linda		
USPTO	Purcell, Art		

OBSERVERS

Organization	Name	Email	Telephone
FPKI	Spencer, Judith		
FPKI OA (Mitretek)	Stern, Michael		
Department of State (ManTech)	Froehlich, Charles R.		
FPKI OA Program Manager	Jenkins, Cheryl		
GSA	Cornell, John		
FICC Support (FC Business Systems)	Petrack, Brant		
DoD PKI PMO	Mitchell, Deborah M.		
Enspier (Secretariat)	Fincher, Judy		
Wells Fargo	Drucker, Peri		
Wells Fargo	Uyeda, Masao		
Wells Fargo	Gross, Jim		
MTS	Tate, Darron		
KPMG	Faut, Nathan		
KPMG	DeVane, DeAndre		

C. MEETING ACTIVITY

Agenda Item 1

Welcome & Opening Remarks / Introductions — Mr. Tim Polk

This meeting took place at the GSA Central Office Building, 1800 F Street, Washington, DC in the basement training room. Mr. Tim Polk, Department of Commerce/NIST and CPWG Co-Chair, called the meeting to order at 10 a.m. with attendee introductions in the absence of the Chair, Dr. Peter Alterman, who was called away unexpectedly. The meeting started late because we were unable to use our regularly scheduled meeting room.

At least one FPKIPA member and observer were unable to join the teleconference because we were not able to establish the teleconference until we found a room. Even then, we used a cell phone with a speaker to support the teleconference.

¹ Ms. Linda Goodwin joined via teleconference after the quorum was established.

Agenda Item 2

Discussion/Vote on Minutes from 13 September FPKIPA meeting — Ms. Judy Fincher

Ms. Fincher described the comments received on the minutes and stated that they had been incorporated as of October 3, 2005. Hardcopies of the redlined document were distributed at the meeting. The revised 13 September 2005 FPKIPA meeting minutes were approved by 8 of those present at the time of the vote, including two proxies, (or 61.5 %), where a simple majority of votes cast was required. One member abstained. These meeting minutes will be posted to the [FPKIPA web site](#) by COB 14 October 2005.

Approval vote for 13 September 2005 FPKIPA Minutes			
Voting members	Vote (Motion –Treasury; 2 nd –USPTO)		
	Yes	No	Abstain
Department of Commerce	X		
Department of Defense	X		
Department of Energy	Absent		
Department of Health & Human Services (Proxy to Commerce)	X		
Department of Homeland Security	Absent		
Department of Justice	Absent		
Department of State	X		
Department of the Treasury	X		
GSA	X		
NASA (Proxy to DoD)	X		
OMB			X
USDA/NFC	Absent		
USPTO	X		

Agenda Item 3

Results of Electronic Voting — Mr. Tim Polk, Ms Judy Fincher

a) Approval Vote for 9 August 2005 FPKIPA Minutes

Electronic Vote. Ten votes were received as of 9-30-05 COB, where a quorum of 9 votes was required. The August 9, 2005 minutes were approved by all those who voted (10 votes) or 100%, where a 50% majority of votes cast is required. The 9 August FPKIPA minutes were posted to the FPKIPA web site on October 3, 2005.

Approval vote for FPKIPA 9 August 2005 Meeting Minutes			
Voting members			
	Yes	No	Abstain
Department of Commerce	X		
Department of Defense	X		
Department of Energy	X		
Department of Health & Human Services	X		
Department of Homeland Security	X		
Department of Justice	Did not Vote		
Department of State	X		
Department of the Treasury	X		
GSA	X		
NASA	X		

OMB	Did not Vote		
USDA/NFC	Did not Vote		
USPTO	X		

b) Approval Vote for EGCA Certificate Policy Change Proposal: 2005-02

Emergency Vote on the EGCA Certificate Policy Change Proposal: 2005-02: Ten affirmative votes were received by COB 9-23-05, where a quorum was 9 votes. The Change Proposal was approved by all who voted (10 votes) or 100%, where a 75% majority of votes cast was required.

Change Proposal 2005-02 modifies the E-Governance CA CP to permit centrally generated key pairs for agency application servers.

Approval vote for EGCA Certificate Policy Change Proposal: 2005-02			
Voting members			
	Yes	No	Abstain
Department of Commerce	X		
Department of Defense	X		
Department of Energy	X		
Department of Health & Human Services	X		
Department of Homeland Security	X		
Department of Justice	Did not Vote		
Department of State	X		
Department of the Treasury	X		
GSA	X		
NASA	X		
OMB	Did not Vote		
USDA/NFC	Did not Vote		
USPTO	X		

c) Approval Vote for Revised Charter

Electronic Vote

Only 5 affirmative votes were received by COB Oct. 3, 2005 where a minimum of nine votes is required for passage. There were three "No" votes. Therefore, the Charter was not approved for adoption by the FPKIPA. No further steps were discussed at the October 11, 2005 meeting to revise the Charter to the satisfaction of the FPKIPA members.

Approval vote for FPKIPA Charter			
Voting members			
	Yes	No	Abstain
Department of Commerce	Did not vote		
Department of Defense		X	
Department of Energy	Did not vote		
Department of Health & Human Services	X		
Department of Homeland Security	X		
Department of Justice	Did not vote		
Department of State	X		
Department of the Treasury	X		
GSA	X		

NASA		X	
OMB	Did not vote		
USDA/NFC	Did not vote		
USPTO		X	

d) Approval Vote for Wells Fargo MOA at Basic LOA

Electronic Vote: Eleven affirmative votes were received as of COB 9/29/05, with two “No” votes, for a total of 13 votes. Where a 75% majority of votes cast was required to approve, there was an 86% majority vote. Wells Fargo’s MOA at Basic LOA was approved.

Approval vote for Wells Fargo MOA at Basic LOA			
Voting members			
	Yes	No	Abstain
Department of Commerce	X		
Department of Defense		X	
Department of Energy	X		
Department of Health & Human Services	X		
Department of Homeland Security	X		
Department of Justice	X		
Department of State	X		
Department of the Treasury	X		
GSA	X		
NASA		X	
OMB	X		
USDA/NFC (Proxy to Dr. Peter Alterman)	X		
USPTO	X		

Agenda Item 4

Approval Vote for the Revised Certificate Profile — Mr. Tim Polk

Mr. Tim Polk presented the revised Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile with a recommendation from the CPWG to adopt the RFC 3647-based FBCA Certificate Policy. He also provided a table showing comments received from DISA, NSA and NASA and their disposition.

Mr. Tim Polk agreed to make several changes to the document to satisfy the concerns of the DoD/Santosh Chokhani in reference to 1) set encoding of naming attributes, 2) pointing to the LDAP portal, 3) and change policy constraints “will be” critical to “should be” critical. Mr. Polk also will change the subject line of the recommendation from the CPWG to reflect the correct name of the document.

Action: Mr. Tim Polk was to make edits to the Certificate Profile document and CPWG recommendation and submit them to Ms. Judy Fincher for an electronic vote.

Action: Mr. Darron Tate is to determine if there is a problem when pointing to the LDAP portal and inform Mr. Tim Polk. If there is a problem, NIST will fix it, according to Mr. Polk.

Agenda Item 5

Approval vote for GPO Cross-Certification at Medium LOA

This item was not voted on due to the reservations expressed by many FPKIPA members as to the credentials of the GPO auditor. The GPO has been asked to provide a curriculum vitae to demonstrate that its auditor has both PKI and auditing experience, a requirement that has been on the FPKIPA web site since February.

There was also discussion, but no prescribed action, to add language to the FPKIPA's audit requirements regarding the use of some formal auditing process, such as SAS 70 or American Institute of Certified Public Accountants (AICPA) WebTrust.

Agenda Item 6

FPKI Certificate Policy Working Group (CPWG) Report — Mr. Tim Polk

- a. Vote to Approve Mapping Wells Fargo at Medium Hardware Commercial Best Practices

Mr. Tim Polk explained that the recommendation being considered for the vote was to map policies, not to cross-certify at Medium Hardware Commercial Best Practices.

Prior to the vote, the FPKIPA members expressed reservations about accepting the mapping because 1) they had not examined the revised Wells Fargo CP/CPS and Authentication Policy to reassure themselves that the appropriate changes had been made, 2) DoD's objection to the liability language in the MOA. The DoD will insist that the MOA language (approved at Basic) be edited.

Action: DoD (Ms. Deborah Mitchell) requested off-line that the revised Wells Fargo CP/CPS and Authentication Policy be circulated to the FPKIPA listserv so that members could examine the revised documents. Ms. Judy Fincher is to obtain the documents and distribute them to the FPKIPA listserv.

The CPWG recommended that the FPKIPA approve mapping Wells Fargo at Medium Hardware Commercial Best Practices and this was not approved by the FPKIPA. There were six "Yes" votes (46%), including three proxies, and three "No" votes where a 75% majority of votes cast was required to approve the mapping.

Approval vote for Mapping Wells Fargo at Medium Hardware Commercial Best Practices			
Voting members	Vote (Motion –GSA; 2nd – State)		
	Yes	No	Abstain
Department of Commerce	X		
Department of Defense		X	
Department of Energy	Absent-Did not vote		
Department of Health & Human Services (Proxy to Department of Commerce)	X		
Department of Homeland Security	Absent-Did not vote		
Department of Justice	Absent-Did not vote		
Department of State	X		
Department of the Treasury	X		
GSA	X		
NASA (Proxy to DoD)		X	
OMB (Proxy to HHS/DOC)	X		
USDA/NFC	Absent-Did not vote		
USPTO		X	

b. Discuss Mapping Adobe in 3647 Format

Mr. Tim Polk explained that the CPWG attempted to map Adobe's CP to the FBCA CP at the Medium LOA without success. There are too many areas that are simply missing or partially documented in the Adobe CP. Adobe would have to make major revisions to their CP and it's probably not worth the effort, Mr. Polk stated. The CPWG will set up a meeting with Adobe to get their agreement to map them at "C4" (Citizen and Commerce Class Certificate Policy).

Conversely, mapping the FBCA CP to Adobe's CP is not a problem. "We meet all their requirements." This is very attractive to the government, since ordinary citizens would be able to confirm the electronic signatures on government documents.

c. Discuss CPWG participation by agencies

Mr. Tim Polk appealed to all FPKIPA members to provide more resources to support the work of the CPWG, which is meeting twice monthly due to its current workload. Mr. Dave Hanco suggested having a fixed date/dates each month would help agencies plan their allocation of resources.

Action: Ms. Judy Fincher is to poll the FPKIPA members on their preferred dates for CPWG meetings, i.e., 2nd and fourth Wednesdays.

Agenda Item 7

FPKI Operational Authority (FPKI OA) Report — Ms. Cheryl Jenkins, Mr. Darron Tate

Status of FBCA/Applicant Cross-Certification Technical Testing (changes in bold)

The DOJ completed interoperability testing and the report has been finalized.

<u>Completed</u>			<u>Current</u>	<u>Future</u>
Dept of the Treasury	Dept of Energy	USPTO		Boeing
NASA	State of Illinois	DHS		Adobe
USDA/NFC	Dept of Labor	HEBCA		USPS
DoD	ACES/DST	Wells Fargo		
DoD KMI	ACES/ORC	GPO		
Government of Canada		DOJ		
DoD ECA	CertiPath			
Dept of State	ACES/AT&T			

Mr. Darron Tate reported on OA activities:

- E-Governance certificates have been issued to: ORC, DOE, SSA and the National Park Service (NPS).
- The Wells Fargo MOA has been signed; now we need to issue the cross-certification.
- The DoD ECA MOA is now under review by John Cornell.
- Ms. Cheryl Jenkins is waiting to receive the Letter of Authorization for cross-certification between the FBCA and ORC. ORC is going to become an SSP.
- There is only one MOA for ACES.

With reference to directory interoperability testing:

- DHS is currently doing directory interoperability testing; the IP's are being dropped and are not reaching the firewall.
- The Department of State has completed directory interoperability testing.

Issues:

The cross-certs for Treasury and NASA will expire the end of October 2005.

Action: Ms. Cheryl Jenkins will send an email to Ms. Judy Fincher regarding an e-vote on the renewal of cross-certificates for Treasury and NASA.

Action: Ms. Cheryl Jenkins will send an email to Ms. Judy Fincher for an e-vote on the acceptance of directory interoperability testing for CertiPath and DOJ.

Mr. Tate stated that the ACES/DST CRL now has an expiration date.

Ms. Cheryl Jenkins stated that the directory architecture at the Department of State is now stable. The DOS will transition to Microsoft Active Directory. The FPKI OA tested with them last week and found the directories to be interoperable. DOS is using Entrust.

Agenda Item 8

Other Topics

a) Wells Fargo Liability Language (context: Medium CBP & Medium Hardware CBP Cross-Certification)

At this juncture three representatives from Wells Fargo joined via teleconference: Ms. Peri Druker, Ms. Jim Gross, and Mr. Masao Uyeda.

Mr. John Cornell summarized the issue at hand. The FPKIPA doesn't usually get involved with the MOA. Mr. Cornell performs a legal review of the MOA to determine if it is violating a statute or regulation. With respect to the "hold harmless" liability language of the Wells Fargo MOA (at Basic LOA), he found that it did not violate statute or regulation. At the Basic LOA the "hold harmless" legal liability language was not an issue. At the Medium CBP and Medium Hardware CBP LOA, the MOA liability language becomes an issue. The ball is now in Wells Fargo's court.

Mr. Jim Gross of Wells Fargo explained that Wells Fargo does accept gross negligence and that the "hold harmless" liability language was intended for the situation where there is two-way interoperability. Currently, there is a one-way flow. Wells Fargo wants to be able to exclude anyone who doesn't meet the Wells Fargo requirement and that was the intention of the liability clause.

Action: Mr. Tim Polk stated that the FPKIPA will take another look at the Wells Fargo liability language and will refine the issues before the next FPKIPA meeting in November.

Mr. Gross also invited the FPKIPA members (Subject Matter Experts) to participate in a new working group being formed by the Electronic Authentication Partnership on the name constraints issue across public and private sectors. Mr. Tim Polk stated that NIST and DoD are also looking into the issue and to keep NIST posted on this activity.

Action: Mr. John Cornell will schedule a meeting between agency lawyers and Wells Fargo legal staff to review legal liability issues. Copies of the "concrete sections of the document" will be distributed prior to the meeting.

b) Document Control

Ms. Cheryl Jenkins and Mr. Brant Petrick are meeting with Enspier, October 13, 2005 to discuss implementation on GSA's server of Document Control modules made available by Enspier. Ms. Jenkins commented that the web-enabled application would make it possible to edit a document during a working group session and then upload the revised document to the server, with revision control statistics.

c) EGCA Certificate Policy Change Proposal: 2005-03 – Distinguished Name

Ms. Cheryl Jenkins reported that this issue was initially thought to be solved by Scott Rea's (Dartmouth) IIS workaround, but now she's looking at it again and will resurrect it in the CPWG.

d) The next FPKIPA Meeting is scheduled for November 8, 2005 (9:30 AM to 12:00 PM at the GSA Central Office Building located at 1800 F Street, Room # 5141A, Washington, DC.

Action Item Review

The action item review was postponed due to time constraints. Members are encouraged to review the action item list in the minutes and notify Ms. Judy Fincher if items have been closed.

Agenda Item 9

Adjourn Meeting

The meeting adjourned at 12:10 p.m.

D. CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
057	Write a short paper that says from here forward the FBCA OA will limit FBCA acceptance testing to systems that demonstrate enhanced assurance through NIAP testing.	Tim Polk, NIST	8 July 2003 Updated – 9 Sept 2003	9 Dec 2003 FPKIPA meeting	Open
062	Define the NIAP certification requirement for future bridge membrane applications.	Tim Polk, NIST	9 Sept 2003	9 Dec 2003 FPKIPA meeting	Open
085	Test/evaluate the PKCS-12 usage issue and make a recommendation to the FPKIPA at a meeting in the near future.	Tim Polk, NIST	13 July 2004	12 October 2004 FPKIPA meeting	Open
112	Update their MOA with the FBCA to reflect the new one-way certificate being issue for the period of January 2005 to January 2006.	DoD	11 Jan 2005	28 Feb 2005	Open
113	Prepare and route a new Letter of Authorization from the FPKIPA to the FPKI OA for this new one-way cross-certificate for the DoD PKI for the period of January 2005 to January 2006.	John Cornell	11 Jan 2005	31 Jan 2005	Open

No.	Action Statement	POC	Start Date	Target Date	Status
FY 05 131	Develop a Compliance Audit Report paper on this issue and report to the FPKIPA at the 14 June FPKIPA meeting.	Cheryl Jenkins, GSA Dave Hanko, DoD	12 Apr 2005	14 June 2005 FPKIPA meeting	Open
134	Mr. John Cornell will contact the DoD lawyer re the status of the DoD ECA MOA.	John Cornell	9 August 2005	13 Sept. 2005	Open
138	Mr. Tim Polk will draft a White Paper before the September 13 FPKIPA meeting, to be distributed after the policy is finished and voted. Agencies need to know the “gap” between RFC 2527 and RFC 3647, since agencies will be required to re-write their CPs.	Tim Polk	9 August 2005	13 Dec. 2005	Open
139	Ms Cheryl Jenkins will help Mr. Polk create a delta matrix table for agencies to use to measure their CPs [delta between RFC 3647 and RFC 2527].	Cheryl Jenkins	9 August 2005	13 Sept. 2005	Open
140	Ms. Jenkins will check with DOE and USPTO regarding using their test labs.	Cheryl Jenkins	9 August 2005	13 Sept. 2005	Open
141	Dr. Alterman noted that we have an audience large (i.e., nationally and internationally) enough for Microsoft to approve it. Dr. Alterman and Ms. Jenkins will meet two weeks from now to review and modify the application’s draft narrative language that will be used to prove that the FPKI audience is large enough.	Dr. Peter Alterman	9 August 2005	13 Sept. 2005	Open
133	All FPKI PA members contact FBCA OA regarding the cost and feasibility of a limited testing environment.	All FPKIPA members	9 August 2005	11 October 2005	Open
136	Mr. Polk will task Mr. David Cooper to test the Adobe software at NIST [using the PKITS test suite for Path Discovery and Validation] by next month and will schedule a meeting with Adobe and the FPKIPA if the testing goes well.	Tim Polk, David Cooper	13 Sept. 2005	11 Oct. 2005	Open
140	Dr. Peter Alterman needs to provide the following MOUs and LOAs to Mr. Darron Tate. <div style="display: flex; justify-content: space-around;"> <div> <u>Organization</u> ORC DoD ECA </div> <div> <u>Need to provide</u> LOA LOA, MOA </div> </div>	Dr. Peter Alterman	13 Sept. 2005	11 Oct. 2005	Open

No.	Action Statement	POC	Start Date	Target Date	Status
	Wells Fargo LOA, MOA				
143	Mr. Tim Polk will schedule a CPWG meeting on the synchronization of the Common Policy, the FBCA Cert Policy and FIPS 201.	Tim Polk	13 Sept. 2005	January 2006	Open
144	Mr. Tim Polk will schedule this topic [frequency in which CAs operating off-line must issue CRL's] for a CPWG meeting.	Tim Polk	13 Sept. 2005	Dec. 2005	Open
145	Ms. Jenkins will send the first draft of the Microsoft application [for the Common Policy Root certificate to be placed into the Microsoft Cert Store] to Ms. Judy Fincher on Friday, Sept. 16, who will forward it to Dr. Peter Alterman.	Cheryl Jenkins	13 Sept. 2005	15 Nov. 2005	Open
147	Dr. Alterman needs to sign both the redacted and clean version of the CPS and post the redacted version to the web site.	Dr. Peter Alterman	13 Sept. 2005	30 Sept. 2005	Open
148	Mr. Tim Polk was to make edits to the Certificate Profile document and CPWG recommendation and submit them to Ms. Judy Fincher for an electronic vote.	Tim Polk	Oct. 11, 2005	Oct. 15, 2005	Open
149	Mr. Darron Tate is to determine if there is a problem when pointing to the LDAP portal and inform Mr. Tim Polk. If there is a problem, NIST will fix it, according to Mr. Polk.	Darron Tate	Oct. 11, 2005	Oct. 15, 2005	Open
150	DoD (Ms. Deborah Mitchell) requested off-line that the revised Wells Fargo CP/CPS and Authentication Policy be circulated to the FPKIPA listserv so that members could examine the revised documents. Ms. Judy Fincher is to obtain the documents and distribute them to the FPKIPA listserv	Judy Fincher	Oct. 11, 2005	Oct. 15, 2005	Open
151	Ms. Judy Fincher is to poll the FPKIPA members on their preferred dates for CPWG meetings, i.e., 2 nd and fourth Wednesdays.	Judy Fincher	11 Oct., 2005	15 Oct. 2005	Open

No.	Action Statement	POC	Start Date	Target Date	Status
152	Ms. Cheryl Jenkins will send an email to Ms. Judy Fincher regarding an e-vote on the renewal of certs for Treasury and NASA.	Cheryl Jenkins & Judy Fincher	11 Oct. 2005	20 Oct. 2005	Open
153	Ms. Cheryl Jenkins will send an email to Ms. Judy Fincher for an e-vote on the acceptance of directory interoperability testing for CertiPath and DOJ.	Cheryl Jenkins & Judy Fincher	11 Oct. 2005	20 Oct. 2005	Open
154	Mr. Tim Polk stated that the FPKIPA will take another look at the Wells Fargo liability language and will refine the issues before the next FPKIPA meeting in November.	Tim Polk & John Cornell	11 Oct. 2005	8 Nov. 2005	Open
155	Mr. John Cornell will schedule a meeting between agency lawyers and Wells Fargo legal staff to review legal liability issues. Copies of the “concrete sections of the document” will be distributed prior to the meeting.	John Cornell	11 Oct. 2005	8 Nov. 2005	Open